AMENDMENTS TO THE CLAIMS

Please amend the claims as indicated in the following listing of all claims:

1. (Currently Amended) A method of securing a data transaction across a security barrier, the method comprising:

validating a request message encoded in a structured request language against a predefined request message specification therefor;

transmitting the validated request message across the security barrier;

validating a response message encoded in a structured response language against a predefined response message specification therefor, the response message corresponding to the validated request; and

transmitting the validated response message across the security barrier,

wherein the predefined request message specification and the predefined response message specification indicate respective message formats specific to one or both of an application and a transaction.

2. (Original) A method as in claim 1,

wherein the request and response message specifications are predefined in accordance with valid request and response message constraints specific to an information resource.

3. (Original) A method as in claim 1,

wherein at least one of the request and response message specifications is cryptographically secured.

4. (Original) A method as in claim 1, further comprising:

receiving, at an application proxy, an access request targeting an information resource;

formatting the request message in a structured language corresponding to the request message specification; and

transmitting the formatted request message to a secure data broker for the request message validating.

5. (Original) A method as in claim 1, further comprising:

formatting the response message in a structured language corresponding to the response message specification; and

transmitting the formatted response message to a secure data broker for the response message validating.

6. (Original) A method as in claim 1, further comprising:

accessing an information resource in accordance with the validated request message; and

preparing the response message in accordance with the access.

7. (Original) A method as in claim 6,

wherein the response message is formatted in a structured language corresponding to the response message specification.

8. (Original) A method as in claim 1,

wherein the request message is formatted in a structured language corresponding to the request message specification; and

wherein the response message is formatted in a structured language corresponding to the response message specification.

9. (Original) A method as in claim 8,

wherein the structured languages corresponding to the request and response message specifications include an eXtensible Markup Language (XML).

10. (Original) A method as in claim 1,

wherein the request and the response message validatings are respectively performed at first and second secure data brokers on opposing sides of the security barrier; and

wherein the validated request and response message transmissions are between the first and second secure data brokers.

11. (Original) A method as in claim 1, wherein the request message validating includes:

parsing the request message using Data Type Definitions (DTDs) encoding a hierarchy of valid tag-value pairs in accordance with syntax of a valid request message; and

if the request message is not successfully parsed, forwarding a response message without transmission of the request message across the security barrier.

12. (Original) A method as in claim 1, wherein the response message validating includes:

parsing the response message using Data Type Definitions (DTDs) encoding a hierarchy of tag-value pairs in accordance with syntax of a valid response message.

13. (Original) A method as in claim 1,

wherein at least one of the validated request message transmitting and the validated response message transmitting is via a secure protocol.

14. (Original) A method as in claim 1,

wherein at least one of the validated request message and the validated response message is encoded in a markup language.

15. (Original) A method as in claim 1,

wherein the security barrier includes a firewall.

16. (Original) A method as in claim 1,

wherein the security barrier includes a secure communication channel between servers.

17. (Original) In a networked computing environment, a method of securing access to an information resource behind a security barrier, the method comprising:

predefining a request message specification corresponding to a structured request language;

formatting an access request in accordance with the structured request language;

supplying the formatted access request to a first intermediary, the intermediary validating the formatted access request in accordance with the request message specification; and

forwarding the validated access request across the security barrier.

18. (Original) A method as in claim 17, further comprising:

accessing the information resource in accordance with the validated access request.

19. (Original) A method as in claim 17, further comprising:

receiving, at an application proxy, an access request targeting the information resource; and

performing the access request formatting at the application proxy.

20. (Original) A method as in claim 17, further comprising:

predefining a response message specification corresponding to a structured response language;

formatting a response to the access request in accordance with the structured language;

supplying the formatted response to a second intermediary, the second intermediary validating the formatted response in accordance with the response message specification; and

forwarding a validated response across the security barrier.

21. (Original) A method as in claim 20, further comprising:

accessing the information resource in accordance with an access request from a client; and

supplying the client with a response in accordance with the validated response.

22. (Original) In a networked computing environment, a method of securing access to an information resource behind a security barrier, the method comprising:

predefining a response message specification corresponding to a structured response language;

formatting a response to an access request targeting the information resource, the formatted response being in accordance with the structured response language;

supplying the formatted response to an intermediary, the intermediary validating the formatted response in accordance with the response message specification; and

forwarding a validated response across the security barrier.

23. (Original) A method as in claim 22, further comprising:

accessing the information resource in accordance with the access request from a client;

supplying the client with a response in accordance with the validated response.

24. (Previously Presented) An information security system comprising:

a security barrier;

a proxy for an information resource, the proxy and the information resource on opposing first and second sides, respectively, of the security barrier;

a data broker on the first side of the security barrier, wherein, in response to an access request targeting the information resource, the data broker validates a request message encoded in a structured request language against a predefined request message specification therefor and forwards only validated request messages across the security barrier.

25. (Original) An information security system as in claim 24, further comprising:

a second data broker on the second side of the security barrier, wherein, in response to an access targeting the information resource, the second data broker validates a response message against a predefined response message specification and forwards only validated response messages across the security barrier.

26. (Original) An information security system as in claim 24, further comprising:

the information resource.

27. (Currently Amended) In a networked information environment including a client and an information resource separated by a security barrier, an information security system comprising:

means for proxying an access request by the client targeting the information resource and for preparing a request message corresponding to the access request in a structured language corresponding to a predefined request message specification;

means for validating the request message against the predefined request message specification and forwarding only validated request messages across the security barrier,

wherein the predefined request message specification indicates a request message format specific to one or both of an application and a transaction.

28. (Original) An information security system as in claim 27, further comprising:

means for validating a response message against a predefined response message specification and forwarding only validated response messages across the security barrier.

29. (Original) An information security system as in claim 27, further comprising:

the security barrier.

30. (Original) A computer program product encoded in computer readable media, the computer program product comprising:

data broker code and parser code executable on a first network server separated from an information resource by a security barrier;

the data broker code including instructions executable as a first instance thereof to receive access requests in a structured language corresponding to a predefined request message specification and to forward validated ones of the access requests across the security barrier toward the information resource; and

the parser code including instructions executable as a first instance thereof to validate the received access requests against the predefined request message specification.

31. (Original) The computer program product of claim 30, further comprising:

an encoding of the predefined request message specification.

32. (Original) The computer program product of claim 30,

wherein the data broker code and parser code are also executable on a second network server separated from a client application by the security barrier;

wherein the data broker code includes instructions executable as a second instance thereof to receive responses in a structured language corresponding to a predefined response message specification and to forward validated ones of the responses across the security barrier toward the client application; and

wherein the parser code includes instructions executable as a second instance thereof to validate the received responses against the predefined response message specification.

33. (original) The computer program product of claim 32, further comprising:

an encoding of the predefined response message specification.

34. (original) The computer program product of claim 30, further comprising:

application proxy code including instructions executable to format the access requests in accordance with the structured language corresponding to the predefined request message specification.

35. (Original) The computer program product of claim 30, encoded by or transmitted in at least one computer readable medium selected from the set of a disk, tape or other magnetic, optical, or electronic storage medium and a network, wireline, wireless or other communications medium.

36. (Previously Presented) The method of claim 1 wherein the structured request language includes a markup language.

37. (Previously Presented) The method of claim 36 wherein the markup language include eXtensible markup language.

38. (Previously Presented) The method of claim 17 wherein the structured request language includes a markup language.

39. (Previously Presented) The method of claim 38 wherein the markup language includes eXtensible markup languge.

40. (Previously Presented) The information security system of claim 24 wherein the structured request language includes a markup language.

41. (Previously Presented) The information security system of claim 40 wherein the markup language includes eXtensible markup language.